

CLAIMS

What is claimed is:

- 1 1. An apparatus comprising:
2 a plurality of modular exponentiators including a first modular exponentiator and
3 a second modular exponentiator; and
4 a coupling device interposed between said first modular exponentiator and said
5 second modular exponentiator to receive a control signal and to selectively couple said
6 first modular exponentiator to said second modular exponentiator in response to a state
7 of said control signal.
- 1 2. The apparatus as set forth in claim 1, said apparatus having a first mode of
2 operation corresponding to a first state of said control signal wherein said first modular
3 exponentiator is operably separated from said second modular exponentiator and a
4 second mode of operation corresponding to a second state of said control signal wherein
5 said first modular exponentiator is operably coupled to said second modular
6 exponentiator via said coupling device.
- 1 3. The apparatus as set forth in claim 2, wherein said first modular exponentiator
2 and said second modular exponentiator operate as two n-bit modular exponentiators in
3 said first mode of operation and as a single 2n-bit modular exponentiator in said second
4 mode of operation, where n is an integer.
- 1 4. The apparatus as set forth in claim 3, wherein n equals 512.
- 1 5. The apparatus as set forth in claim 1, wherein each of said plurality of modular
2 exponentiators comprises a modular multiplier to perform a modular multiplication of
3 the form $A \times B \bmod M$, where A, B, and M are all integers.
- 1 6. The apparatus as set forth in claim 5, wherein said modular multiplier comprises
2 a Montgomery multiplier.

1 7. The apparatus as set forth in claim 5, wherein said modular multiplier comprises
2 a systolic array of processing elements.

1 8. The apparatus as set forth in claim 1, wherein said a coupling device comprises a
2 multiplexer.

1 9. An apparatus comprising:
2 a plurality of modular multipliers including a first modular multiplier and a
3 second modular multiplier;
4 a coupling device interposed between said first modular multiplier and said
5 second modular multiplier to receive a control signal and to selectively couple said first
6 modular multiplier to said second modular multiplier in response to a state of said
7 control signal.

1 10. The apparatus as set forth in claim 9, said apparatus having a first mode of
2 operation corresponding to a first state of said control signal wherein said first modular
3 multiplier is operably separated from said second modular multiplier and a second mode
4 of operation corresponding to a second state of said control signal wherein said first
5 modular multiplier is operably coupled to said second modular multiplier via said
6 coupling device.

1 11. The apparatus as set forth in claim 10, wherein said first modular multiplier and
2 said second modular multiplier operate as two n-bit modular multipliers in said first
3 mode of operation and as a single 2n-bit modular multiplier in said second mode of
4 operation, where n is an integer.

1 12. The apparatus as set forth in claim 11, wherein n equals 512.

1 13. The apparatus as set forth in claim 9, wherein each of said plurality of modular
2 multipliers comprises a Montgomery multiplier.

1 14. The apparatus as set forth in claim 9, wherein each of said plurality of modular
2 multipliers comprises a systolic array of processing elements.

1 15. The apparatus as set forth in claim 9, wherein said a coupling device comprises a
2 multiplexer.

1 16. A processor comprising:
2 a plurality of modular exponentiators including a first modular exponentiator and
3 a second modular exponentiator; and
4 a coupling device interposed between said first modular exponentiator and said
5 second modular exponentiator to receive a control signal and to selectively couple said
6 first modular exponentiator to said second modular exponentiator in response to a state
7 of said control signal.

1 17. The processor as set forth in claim 16, said processor having a first mode of
2 operation corresponding to a first state of said control signal wherein said first modular
3 exponentiator is operably separated from said second modular exponentiator and a
4 second mode of operation corresponding to a second state of said control signal wherein
5 said first modular exponentiator is operably coupled to said second modular
6 exponentiator via said coupling device.

1 18. The processor as set forth in claim 17, wherein said first modular exponentiator
2 and said second modular exponentiator operate as two n-bit modular exponentiators in
3 said first mode of operation and as a single 2n-bit modular exponentiator in said second
4 mode of operation, where n is an integer.

1 19. The processor as set forth in claim 18, wherein n equals 512.

1 20. The processor as set forth in claim 16, wherein said a coupling device comprises
2 a multiplexer.

1 21. A system comprising:
2 a memory to store data and instructions;
3 a first processor coupled to said memory to process data and execute instructions;
4 and
5 a second processor coupled to said memory, said second processor comprising:
6 a plurality of modular exponentiators including a first modular
7 exponentiator and a second modular exponentiator; and
8 a coupling device interposed between said first modular exponentiator and
9 said second modular exponentiator to receive a control signal and to selectively
10 couple said first modular exponentiator to said second modular exponentiator in
11 response to a state of said control signal.

1 22. The system as set forth in claim 21, said second processor having a first mode of
2 operation corresponding to a first state of said control signal wherein said first modular
3 exponentiator is operably separated from said second modular exponentiator and a
4 second mode of operation corresponding to a second state of said control signal wherein
5 said first modular exponentiator is operably coupled to said second modular
6 exponentiator via said coupling device.

1 23. The system as set forth in claim 22, wherein said first modular exponentiator and
2 said second modular exponentiator operate as two n-bit modular exponentiators in said
3 first mode of operation and as a single 2n-bit modular exponentiator in said second mode
4 of operation, where n is an integer.

1 24. A method comprising:
2 receiving a control signal;
3 selectively coupling a first modular exponentiator to a second modular
4 exponentiator of a plurality of modular exponentiators in response to a state of said
5 control signal;
6 receiving a plurality of operands; and

7 performing a modular exponentiation operation on said plurality of operands
8 utilizing said first modular exponentiator and said second modular exponentiator.

1 25. The method as set forth in claim 24, wherein selectively coupling a first modular
2 exponentiator to a second modular exponentiator of a plurality of modular exponentiators
3 in response to a state of said control signal comprises:

4 operably separating said first modular exponentiator from said second modular
5 exponentiator in a first mode of operation corresponding to a first state of said control
6 signal; and

7 operably coupling said first modular exponentiator to said second modular
8 exponentiator in a second mode of operation corresponding to a second state of said
9 control signal.

1 26. The method as set forth in claim 25, wherein performing a modular
2 exponentiation operation on said plurality of operands utilizing said first modular
3 exponentiator and said second modular exponentiator comprises:

4 operating said first modular exponentiator and said second modular exponentiator
5 as two n-bit modular exponentiators in said first mode of operation and as a single 2n-bit
6 modular exponentiator in said second mode of operation, where n is an integer.

1 27. A machine-readable medium having a plurality of machine-executable
2 instructions embodied therein which when executed by a machine, cause said machine to
3 perform a method comprising:

4 receiving a control signal;

5 selectively coupling a first modular exponentiator to a second modular
6 exponentiator of a plurality of modular exponentiators in response to a state of said
7 control signal;

8 receiving a plurality of operands; and

9 performing a modular exponentiation operation on said plurality of operands
10 utilizing said first modular exponentiator and said second modular exponentiator.

1 28. The machine-readable medium as set forth in claim 27, wherein selectively
2 coupling a first modular exponentiator to a second modular exponentiator of a plurality
3 of modular exponentiators in response to a state of said control signal comprises:
4 operably separating said first modular exponentiator from said second modular
5 exponentiator in a first mode of operation corresponding to a first state of said control
6 signal; and
7 operably coupling said first modular exponentiator to said second modular
8 exponentiator in a second mode of operation corresponding to a second state of said
9 control signal.

1 29. The machine-readable medium as set forth in claim 28, wherein performing a
2 modular exponentiation operation on said plurality of operands utilizing said first
3 modular exponentiator and said second modular exponentiator comprises:
4 operating said first modular exponentiator and said second modular exponentiator
5 as two n-bit modular exponentiators in said first mode of operation and as a single 2n-bit
6 modular exponentiator in said second mode of operation, where n is an integer.